	APOLLO HOSPITALS,SECUNDERABAD	IMS – 05b Issue: C
	POLICY ON DATA STORAGE AND RETRIEVAL	Date: 06-01-2017 Page 1 of 7
PREPARED BY: HOD-IT	APPROVED BY: Chief Executive Officer	

DATA STORAGE AND RETRIEVAL

Policy for storage, retrieval, Safeguarding data record against loss, destruction and tampering

1. The organization determines the need for and appropriate levels of security and confidentiality of data and information.
2. The organization determines how data and information can be retrieved on a timely and easy basis without compromising the data's and information's security and confidentiality.
3. The organization has a functioning mechanism designed to preserve the confidentiality of data and information identified as sensitive or requiring extraordinary means to protect patient privacy.
4. The organization has a functioning mechanism designed to safeguard records and information against loss, destruction, tampering, and unauthorized access or use.

This section addresses issues regarding confidentiality, security and integrity of the data.

In particular, meeting the intent of this standard requires achieving a balance between the need to provide personnel with access to the information they need and the need to ensure confidentiality of the information.

The management of these issues addresses who has access to what information, the obligations of personnel with respect to confidentiality, the release of medical records, and the mechanisms for guarding against unauthorized intrusion, corruption, and damage.

Many of the requirements in this section are not new; however, they have been broadened to include all types of data and information (i.e., human resource, credentialing, and risk management information).

The organization determines the need for and appropriate levels of security and confidentiality of data and information.

In general, the facility should have policies and procedures in place and implemented, at both the organization-wide level and the departmental level, regarding security and confidentiality of information. The organization, through terminals and printers located throughout the organization, provides easy access to information; system security should be an integral part of the overall security plan.

Security features offer the following capabilities to be leveraged in the security portion of the information management plan:

- Assignment of access through the use of user groups based on need for/use of the information.
- Automatic maintenance of the verify code, with the site having ability to set.
- Audit trail reports at the Digital Standard AND Virtual Memory System (VMS), levels to monitor and control access.

Ad hoc reports can also be used to assemble data on particular access issues.

For facilities that have implemented the Inpatient Divided Work Center, information access can be restricted to a user's division while granting access for other users who need access to integrated patient information across divisions.

The audit trail reports provide information on who changed agreements, what the changes were, when the changes were made, etc., by different categories (e.g., group agreements, single provider).

The system can assist in the dissemination of policies and procedures regarding security and access through the use of software combined with the View Text feature of Clinical Desktop.

The organization determines how data and information can be retrieved on a timely and easy basis without compromising the data's [sic] and information's security and confidentiality.

Through the distribution of terminals in patient care, administrative, ancillary, and support areas throughout the facility, and through the system design feature that allows any authorized user to access information from any terminal, regardless of location, the organisation provides timely and easy access to the information collected and maintained in the system. Users can obtain printed copies of data outputs and reports upon request or as part of routine printing cycles.

The system also offers features and reports that can be used in the process of monitoring and controlling access, and in investigating unauthorized access or other security violations.

Ad hoc reports can also be developed to monitor dial-in access or research any reported breach in security.

The organization has a functioning mechanism designed to preserve the confidentiality of data and information identified as sensitive or requiring extraordinary means to protect patient privacy.

Through the display of the Privacy Act Statement on appropriate Screens and outputs, users are reminded of the sensitive nature of the data and the need to protect confidentiality

Through the security features of the system, site personnel can control access to data in the following ways:

- Limit access to specific menus and pathways.
- Control access to the data element level.

Capabilities for providing extra protection against unauthorized access to sensitive information include the following:

- Limit access to data/information on highly sensitive (Very Important Person [VIP]) patients.
- Limit access to credentialing information.
- Limit access to sensitive patient information such as laboratory test results for Human Immunodeficiency Virus (HIV), sexually transmitted diseases, etc., or appointments for mental health services to designated personnel with need to know.

For HIV and other sensitive test results, the system also provides a report--Sensitive Results Access List (LAB)--listing all users who accessed sensitive results.

For facilities that have implemented Inpatient Divided Work Center, system capabilities include the ability to limit access to users within same division.

The option for the Consultation Form includes three additional security keys whereby the facility can control access to consultation reports for VIPs, patients with HIV, and other sensitive cases (e.g., patients under psychiatric care).

4. The organization has a functioning mechanism designed to safeguard records and information against loss, destruction, tampering, and unauthorized access or use.

The overall implementation and day-to-day operations of the organization have mechanisms designed to safeguard data/information against loss destruction, and unauthorized access or use. Many of these mechanisms are specified in the System Security Plan and the Contingency of Operations Plan. Some of the primary mechanisms are likely to include:

- System back-up on a routine daily / weekly basis and a remote backup to be kept in different place.
- Uninterruptible power supply to protect from power outages planned testing of emergency power, etc.
- Archiving of data and the storage of the data in a location with appropriate physical security (controlled access, fire-proof vaults, protection from water damage, etc.).
- Communication through Intercom notification of user need to change verify code at site-defined periods of time.

- Yearly modification of the user access code as and when required.
- Plan for recovering important data and information in the event of a disaster.
- The system has two sets of hard drives. One set runs the system and the second set serves as a copy(mirror). This means that all information is duplicated in the system to minimize data loss from a system crash.

- The system is backed up on external hard drive every 24 hours. The external hard drive are stored in the Information Technology / Telemedicine Department and it is available when the system fail.
- Daily back up into external hard drive are stored in a fireproof safe in the Information Technology Department.

Contingency procedures for operations interruptions

Anticipated system down time is scheduled for hours of lowest impact. (Examples include night shift and lunch time.) Departments are given advance notice of scheduled system down time over intercom.

Each department has procedures for management of information during computer down time.

Emergency Management Plan :

Each department has procedures for management of information during computer down time.

Each department has a Utilities Management Plan for emergencies.

DATA RETRIEVAL:

- Data retrieval and what it will address, including retrieval from storage and information presently in the system, retrieval of data in the event of system interruption, and back up of data
- Daily back up of the system is performed and information stored on external hard drive. These external hard drives are available to retrieve data in the event of a system failure.
- The system has two hard drives that mirror data to decrease the likelihood of a system failure.
- In the event of a system interruption, each department has procedures for the management of information and a department specific Utilities Management Plan for emergencies.
- As there is a constraint in Hardware and software limitation, the online data is kept for one year and all the other Data is kept offline. The offline data is adequately kept in the back up server and can be accessed on demand. The Offline data can be provided on demand within 24 hrs of the requested time.

SAFEGUARDING

- Ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information;
- Limit the sharing of information that identifies individuals or contains proprietary information to that which is authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists;
- Provide individuals, upon request, access to records about them maintained in Privacy Act systems of records.